UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/994,476	11/26/2001	Ari Juels	1048-016	7236

47653 7590 06/06/2008

BAINWOOD HUANG AND ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
06/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/994,476	JUELS ET AL.	
	Examiner	Art Unit	
	JEFFERY WILLIAMS	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 2, 4 – 28, and 38 – 45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9 and 10* is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 3/5/08.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 2, 4 – 28, and 38 – 45 are pending.

Claim Objections

Claim 16 is objected to for being dependent upon a rejected claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 38 and 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Regarding claims 38 and 39, these claims comprise essentially computer instructions upon a readable medium such as carrier waves. As such, such claims are rejected for not being tangible.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 4 – 8, 11, 12, 14 – 15, 17 – 28, and 38 – 45 are rejected under 35 U.S.C. 102(b) as being anticipated by Juels et al. (Juels), "A Fuzzy Commitment Scheme".

Regarding claim 1, Juels discloses:

(a) receiving a first input element comprising a sequence of a least one value $(a_1, \ldots, a_n)$ *from a predetermined set* (pg. 32-33, "example 2", par. 2);

(b) generating a codeword of an error-correcting code for generating the commitment (pg. 32-33, "example 2", par. 1, 2);

(c) constructing a first sequence of coordinate sets (x_i, y_i)*, for i in {1,...n}, each of the coordinate sets having a first value* (x_i) *corresponding to a representation of an associated one* (a_i) *of the at least one value of the first input element and a second value* (y_i) *corresponding to a symbol in the codeword, wherein the symbol corresponds to the* x_i*th symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the commitment having the property that it may be algorithmically combined*

with at least one set of values comprising at least one value of the first input element so as to yield the codeword (pg. 32-33, "example 2", par. 2).

outputting the first sequence (pg. 32-33, "example 2", par. 2 – the sequence is stored).

Regarding claim 2, Juels discloses:

wherein the representation of the first value in the first sequence of coordinate set is an integer representation (pg. 31, section 4.1, par. 1).

Regarding claims 4 and 5, Juels discloses deriving the first input element from biometric measurements (pg. 29, section 2.1).

Regarding claims 6 – 8, Juels discloses:

adding chaff to the first sequence, further including adding the chaff as sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is generated at random; further including adding the chaff as sets of pairs of the form (x,y) such that one or more values x do lie in the input sequence and y is generated at random (pg. 31, section 3.1, par. 3, section 4.1, par. 2; pg. 32, col 1, par. 1,2).

Regarding claim 11, Juels discloses:

further including applying a bijective function to an input secret to obtain the codeword for the symbol corresponding to the second value (pg. 30, section 3, par. 3).

Regarding claim 12, Juels discloses:

receiving a second input element including a second sequence of a least one value ($b_{1,}$…, b_m) from the predetermined set; receiving the first sequence (pg. 32, col. 2, "x" " x' ");

constructing a derived set of values (X'= x_1',…, $x_{m'}$) representing respectively the at least one value ($b_{1,}$…, b_m) in the second sequence; selecting a subset of the coordinate sets {(xi, yi)} in the first sequence (E) such that for each pair (x', y') in the subset, the first value in the pair (x') lies in the derived set of values (X') (pg. 32, col. 1, par. 2-4; pg. 32-33, "example 2");

applying an error-correcting function to the subset (pg. 32, col. 1, par. 3,4).

Regarding claims 13, Juels discloses:

wherein the error-correcting function includes a Reed-Solomon code (pg. 34, col. 2).

Regarding claim 14, Juels discloses:

selecting a polynomial to generate the codeword (pg. 32, "example 2"; pg. 33, section 5.1).

Regarding claims 15, Juels discloses:

utilizing a decodable design for decommitting the order-invariant commitment (pg. 34, section 5.2).

Regarding claims 17 – 28, and 38 – 45, they comprise essentially similar limitations, and they are rejected, at least for the same reasons as the claims above.

Response to Arguments

Applicant's arguments filed 3/5/08 have been fully considered but they are not persuasive.

Applicant argues essentially that:

(i) *Further, what is produced in Example 2 is not a sequence of coordinate sets, as claimed. Applicant respectfully points out that it appears that the Examiner may be trying to identify the pair (α, 8) as a coordinate pair. However, α is a hash value and does not point to a symbol in the codeword as required by claim 1.* (Remarks, pg. 15, par. 3)

In response, the examiner respectfully notes that the prior art discloses a coordinate pair F (c, x), wherein c corresponds to a symbol in the codeword (Juels, pg. 33, col. 1, par. 2).

(ii) *The difference between x and x' is within the correction threshold of the error correcting code to allow successful decommitment. However, the commitment in Example 2 of Juels is not order invariant, as claimed.* (Remarks, pg. 15, par. 1)

In response, the examiner respectfully notes that the applicant's recitation "wherein an order-invariant fuzzy commitment is formed" is merely descriptive language and is not a limiting method step within the method of claim 1. It appears according to the applicant's assertions, that the method steps of a ("receiving a first input…"), b ("generating a codeword…"), and c ("constructing a first sequence of coordinate

sets…") results in the described "order-invariant fuzzy commitment" - there being no further steps necessary for creating order invariance beyond the recited steps of a, b, and c (Remarks, pg. 14, lines 1-8). As, the prior art clearly discloses the method steps of "receiving…", "generating a codeword…", and "constructing a first sequence of coordinate sets…", then the examiner maintains that the prior art discloses the claim limitations of claim 1 which are asserted by the applicant to result in order invariance.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFERY WILLIAMS whose telephone number is (571)272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137